Cyclicity of $\mathbb{U}$

Manu Anish, Carol Bao

ROSS Mathematics Program

July 2023

"Young man, in mathematics you don't understand things, you just get used to them."

— *Neumann*

What is $\mathbb{U}$?

Definition ($\mathbb{U}_m$)

Define $\mathbb{U}_m$ to be the multiplicative group of elements that have an inverse in $\mathbb{Z}_m$.

What is $\mathbb{U}_{16}$?

Definition ($\mathbb{U}_m$)

Define $\mathbb{U}_m$ to be the multiplicative group of elements that have an inverse in $\mathbb{Z}_m$.

Examples

1. $\mathbb{U}_{16} =$
2. $\mathbb{U}_{17} =$
3. $\mathbb{U}_{69} =$

What is $\mathbb{U}_{17}$?

Definition ($\mathbb{U}_m$)

Define $\mathbb{U}_m$ to be the multiplicative group of elements that have an inverse in $\mathbb{Z}_m$.

Examples

1. $\mathbb{U}_{16} = \{1, 3, 5, 7, 11, 13, 15\}$
2. $\mathbb{U}_{17} =$
3. $\mathbb{U}_{69} =$

What is $\mathbb{U}_{69}$?

Definition ($\mathbb{U}_m$)

Define $\mathbb{U}_m$ to be the multiplicative group of elements that have an inverse in $\mathbb{Z}_m$.

Examples

1. $\mathbb{U}_{16} = \{1, 3, 5, 7, 11, 13, 15\}$
2. $\mathbb{U}_{17} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
3. $\mathbb{U}_{69} =$

What is $\mathbb{U}_{69}$?

Definition ($\mathbb{U}_m$)

Define $\mathbb{U}_m$ to be the multiplicative group of elements that have an inverse in $\mathbb{Z}_m$.

Examples

1. $\mathbb{U}_{16} = \{1, 3, 5, 7, 11, 13, 15\}$
2. $\mathbb{U}_{17} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
3. $\mathbb{U}_{69} =$
   $\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 25, 26, 28, 29, 31, 32, 34, 35, 37, 38, 40, 41, 43, 44, 47, 49, 50, 52, 53, 55, 56, 58, 59, 61, 62, 64, 65, 67, 68\}$

What is $\mathbb{U}_{69}$?

Definition ($\mathbb{U}_m$)

Define $\mathbb{U}_m$ to be the multiplicative group of elements that have an inverse in $\mathbb{Z}_m$.

Examples

1. $\mathbb{U}_{16} = \{1, 3, 5, 7, 11, 13, 15\}$
2. $\mathbb{U}_{17} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
3. $\mathbb{U}_{69} = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 25, 26, 28, 29, 31, 32, 34, 35, 37, 38, 40, 41, 43, 44, 47, 49, 50, 52, 53, 55, 56, 58, 59, 61, 62, 64, 65, 67, 68\}$

Lemma 0

$|\mathbb{U}_p| = \varphi(p)$

Orders

Definition ($\mathrm{ord}_m(a)$)

The function $\mathrm{ord}_m(a)$ calculates the order of an element a in the group, which is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. In other words, $\mathrm{ord}_m(a) = k$

Orders

Definition ($\mathrm{ord}_m(a)$)

The function $\mathrm{ord}_m(a)$ calculates the order of an element a in the group, which is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. In other words, $\mathrm{ord}_m(a) = k$

Examples

- $\mathrm{ord}_7(3) =$

Examples of Orders

Definition ($\mathrm{ord}_m(a)$)

The function $\mathrm{ord}_m(a)$ calculates the order of an element a in the group, which is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. In other words, $\mathrm{ord}_m(a) = k$

Examples

- $\mathrm{ord}_7(3) = 6$

$$3^1 \equiv 1 \pmod{7} \quad 3^3 \equiv 6 \pmod{7} \quad 3^5 \equiv 5 \pmod{7}$$

$$3^2 \equiv 2 \pmod{7} \quad 3^4 \equiv 4 \pmod{7} \quad 3^6 \equiv 1 \pmod{7}$$

So the order of 3 in $\mathbb{U}_7$ is 6.

Remark

$\mathrm{ord}_m(n)$ is only defined when $\gcd(m, n) = 1$ (due to Bezout)

Lemma 18

If $\mathrm{ord}_m(a) = r$ and $\mathrm{ord}_m(b) = s$ and $\gcd(r, s) = 1$, then $rs = \mathrm{ord}_m(ab)$

Generators

Definition

We say an element a is a generator of $\mathbb{U}_m$ if every element in $\mathbb{U}_m$ can be expressed in the form a^k, where $k \in \mathbb{Z}^+$.

Generators

Definition

We say an element a is a generator of $\mathbb{U}_m$ if every element in $\mathbb{U}_m$ can be expressed in the form a^k, where $k \in \mathbb{Z}^+$.

Examples

- Is 3 a generator in $\mathbb{U}_7$?

Examples of Generators

Definition

We say an element a is a generator of $\mathbb{U}_m$ if every element in $\mathbb{U}_m$ can be expressed in the form a^k, where $k \in \mathbb{Z}^+$.

Examples

- Is 3 a generator in $\mathbb{U}_7$?

$$\begin{array}{lll} 3^1 \equiv 1 \pmod 7 & 3^3 \equiv 6 \pmod 7 & 3^5 \equiv 5 \pmod 7 \\ 3^2 \equiv 2 \pmod 7 & 3^4 \equiv 4 \pmod 7 & 3^6 \equiv 1 \pmod 7 \end{array}$$

3 is a generator as shown from the list of congruences, it can generate all elements of $\mathbb{U}_7 = \{1, 2, 3, 4, 5, 6\}$

Cyclicity

Definition

$\mathbb{U}_m$ is cyclic if there exists a generator in $\mathbb{U}_m$.

Cyclicity

Definition

$\mathbb{U}_m$ is cyclic if there exists a generator in $\mathbb{U}_m$.

Examples

- Is $\mathbb{U}_7$ cyclic?

Cyclicity

Definition

$\mathbb{U}_m$ is cyclic if there exists a generator in $\mathbb{U}_m$.

Examples

- Is $\mathbb{U}_7$ cyclic?

  Yes, $\mathbb{U}_7$ is cyclic since there exists a generator: namely, 3, such that it can generator all the elements in the group.

So... when is $\mathbb{U}_m$ cyclic?

m	$\mathbb{U}_m$	$\max(\mathrm{ord}_m(a) \mid a \in \mathbb{U}_m)$
1	[]	1
2	[1]	1
3	[1, 2]	2
4	[1, 3]	2
5	[1, 2, 3, 4]	4
6	[1, 5]	2
7	[1, 2, 3, 4, 5, 6]	6
8	[1, 3, 5, 7]	2
9	[1, 2, 4, 5, 7, 8]	6
10	[1, 3, 7, 9]	4
11	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]	10
12	[1, 5, 7, 11]	2
13	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]	12
14	[1, 3, 5, 9, 11, 13]	6
15	[1, 2, 4, 7, 8, 11, 13, 14]	4

Patterns in $\mathbb{U}_m$

m	$\mathbb{U}_m$	$\max(\mathrm{ord}_m(a) \mid a \in \mathbb{U}_m)$
1	[]	1
2	[1]	1
3	[1, 2]	2
4	[1, 3]	2
5	[1, 2, 3, 4]	4
6	[1, 5]	2
7	[1, 2, 3, 4, 5, 6]	6
8	[1, 3, 5, 7]	2
9	[1, 2, 4, 5, 7, 8]	6
10	[1, 3, 7, 9]	4
11	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]	10
12	[1, 5, 7, 11]	2
13	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]	12
14	[1, 3, 5, 9, 11, 13]	6
15	[1, 2, 4, 7, 8, 11, 13, 14]	4

Conjectures!

Given the patterns here are some conjectures we can form:

- when m is prime then, $\mathbb{U}_m$ is cyclic
- when m is p^k where p is an odd prime then, $\mathbb{U}_m$ is cyclic
- when m is $2 \cdot p^k$ where p is an odd prime then, $\mathbb{U}_m$ is cyclic
- when m is 4 then, $\mathbb{U}_m$ is cyclic

$\mathbb{U}_m$ and connections to $\mathbb{Z}_m[x]$...

To prove our conjectures, we take a slight detour into the ring of polynomials modulo m. For the sake of brevity and conciseness we will be using the following theorems/lemmas to aid us (without proof):

1. (UFT) If $f(x)$ is an element of $\mathbb{Z}m[x]$ and has degree n, then $f(x)$ has at most n distinct roots
2. (Euler's Theorem) All units satisfy the equation $x^{\varphi(m)} - 1 \equiv 0 \mod m$
3. If $f(x) = p(x)q(x)$, then the set of roots of $p(x)$ are a subset of the set of roots of $f(x)$

Proof that $\mathbb{U}_p$ is cyclic

Let a be the generator of Up. Up is cyclic when $\mathrm{ord}_p(a) = \varphi(p) = p - 1$. In addition, by Euler's totient theorem, all units satisfy the equation $x^{p-1} - 1 \equiv 0 \mod m$. Let,

$$p - 1 = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}.$$

Therefore,

$$p_i^{e_i} | p - 1 \iff x^{p_i^{e_i}} - 1 | x^{p-1} - 1$$

Proof that $\mathbb{U}_p$ is cyclic (continued)

Since,

$$p_i^{e_i} | p - 1 \iff x^{p_i^{e_i}} - 1 | x^{p-1} - 1$$

and,

$$p_i^{e_i - 1} | p_i^{e_i} \iff x^{p_i^{e_i} - 1} - 1 | x^{p_i^{e_i}} - 1$$

The roots of $x^{p_i^{e_i} - 1} - 1$ is a subset of the roots of $x^{p_i^{e_i}} - 1$, which is also a subset of the roots of $x^{p-1} - 1$.

Proof that $\mathbb{U}_p$ is cyclic (continued)

$x^{p_i^{e_i}} - 1$ has $p_i^{e_i}$ distinct roots with order $1, p_i, p_i^2, \ldots, p_i^{e_i}$ because the orders must divide $p_i^{e_i}$

$x^{p_i^{e_i}-1} - 1$ has $p_i^{e_i} - 1$ distinct roots with order $1, p_i, p_i^2, \ldots, p_i^{e_i-1}$ because the orders must divide $p_i^{e_i-1}$

So, of the $p_i^{e_i}$ roots, the number of roots with order $p_i^{e_i}$ is $p_i^{e_i} - p_i^{e_i-1}$

This means that it is always possible to find an element in $\mathbb{U}_p$ that has order $p_i^{e_i}$ for all $i \in \mathbb{Z}^+$

Proof that $\mathbb{U}_p$ is cyclic (continued)

Let $a_1, a_2, \ldots, a_n$ be the units with order $p_1^{e_1}, p_2^{e_2}, \ldots p_n^{e_n}$ respectively. $p_1^{e_1}, p_2^{e_2}, \ldots p_n^{e_n}$ are all coprime with each other.

$$\begin{aligned} p-1 &= p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n} \\ &= \mathrm{ord}_p(a_1) \times \mathrm{ord}_p(a_2) \ldots \mathrm{ord}_p(a_n) \\ &= \mathrm{ord}_p(a_1 a_2) \times \mathrm{ord}_p(a_3) \ldots \mathrm{ord}_p(a_n) \\ &= \mathrm{ord}_p(a_1 a_2 a_3) \times \mathrm{ord}_p(a_4) \ldots \mathrm{ord}_p(a_n) \\ &= \mathrm{ord}_p(a_1 a_2 \ldots a_n) \end{aligned}$$

Since $\mathbb{U}_p$ is closed under multiplication, $a_1 a_2 \ldots a_n$ is an element of $\mathbb{U}_p$, more specifically, it is a generator of $\mathbb{U}_p$. Therefore, $\mathbb{U}_p$ is cyclic.

Proof that $\mathbb{U}_{p^k}$ is cyclic

Let $u \in \mathbb{U}_{p^k}$. u is a generator if $\text{ord}(u) = \varphi(p^k)$.

$$\begin{aligned}\varphi(p^k) &= p^k(1 - \frac{1}{p}) \\ &= p^{k-1}(p-1) \\ &= p^{k-1}(p_1^{e_1} p_2^{e_2} \dots p_n^{e_n})\end{aligned}$$

Consider $x^{\varphi(p^k)} - 1.$, Similar to the proof of before, we can show that there are units with order $p_1^{e_1}, p_2^{e_2}, \dots p_n^{e_n}$. Multiplying these units will allow us to construct a generator, proving that $\mathbb{U}_{p^k}$ is cyclic.

Proof that $\mathbb{U}_{2p^k}$ is cyclic

Using a similar argument previously, we find that

$$\begin{aligned}\varphi(2p^k) &= 2p^k(1 - \frac{1}{2})(1 - \frac{1}{p}) \\ &= p^{k-1}(p-1) \\ &= \varphi(p^k)\end{aligned}$$

This means that $\mathbb{U}_{p^k}$ and $\mathbb{U}_2p^k$ are isomorphic. Then since $\mathbb{U}_{p^k}$ is cyclic; therefore, $\mathbb{U}_2p^k$ is cyclic.